IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS, in her official capacity, Defendant.	Civil Action No. 1:20-cv-12090

MEMORANDUM IN SUPPORT OF ATTORNEY GENERAL'S
EMERGENCY MOTION TO COMPEL PRODUCTION OF DOCUMENTS

The 2020 Massachusetts Right to Repair Law requires certain vehicles sold in the Commonwealth to come equipped with a "platform" capable of providing access to "all mechanical data" pertaining to that vehicle. The plaintiff, an automobile industry trade group, has filed this suit to prevent that law from going into effect, alleging that it is impossible for automobile manufacturers to comply with the law while also complying with the federal Motor Vehicle Safety Act and Clean Air Act. Specifically, the plaintiff contends that equipping vehicles with a data-access platform as required by the 2020 Right to Repair Law will necessarily require manufacturers to compromise electronic cybersecurity features built into the design and architecture of their vehicles.

As directed by the Court, see ECF #79 at 5,8,16-17, the plaintiff has designated four manufacturers—General Motors, Fiat Chrysler Automobiles (FCA), Mercedes-Benz, and Toyota—to present evidence in support of that contention. And, since shortly after discovery began, the Attorney General has diligently sought production of documents—specifically,

technical documents that detail the electronic and security design, architecture, and functioning of a small number of makes/models—necessary to test that contention and allow the Attorney General's experts to evaluate whether manufacturers can safely comply with the 2020 Right to Repair Law. In view of this case's expedited, 13-week discovery schedule, as well as the sheer technical complexity of these issues, the Attorney General is extremely mindful that time is of the essence.

Last Friday, however, about 6 weeks after the Attorney General requested those technical documents, the plaintiff unilaterally declared that many of them would not be produced, but rather would be made available for inspection on an "eyes only" basis at physical locations in Michigan.[1] The plaintiff also declared that many other documents would not be produced in any form, on the ground that they are "owned" by Toyota's and Mercedes-Benz's foreign affiliates. And the plaintiff declared its production to be complete, even though documents that had been produced support the existence of other responsive documents that have not been produced.

The Attorney General now seeks the following relief:

1. An order compelling the production to the Attorney General of all responsive documents that the plaintiff has proposed to make available only in Michigan and/or only on an "eyes only" basis;

2. An order compelling the production of documents that are claimed to be beyond the possession, custody, and control of Toyota and Mercedes-Benz;

3. An order compelling the production of responsive reports of security reviews that apparently have not been produced; and

4. An order extending the Attorney General's deadline to serve expert disclosures to a date seven days after the plaintiff completes its production of these critical technical documents.

---

[1] The plaintiff also declared that some documents would be made available on an "eyes only" basis at an electronic location.

FACTS

The plaintiff's central claim is that, to comply with the 2020 Right to Repair Law, manufacturers have no choice but to "eliminate existing cybersecurity controls that protect core vehicle functions and thereby ensure the safe operation of vehicles within prescribed emissions limits." ECF #27 at 7. After the Attorney General voiced her concern that the factual issues bound up in that claim "appear to vary based on specific manufacturer and vehicle model," ECF #63 at 2, this Court instructed the plaintiff to designate up to five manufacturers to provide evidence and participate in discovery "as if they were parties . . . ." ECF #79 at 17. The plaintiff subsequently designated General Motors, FCA, Mercedes-Benz, and Toyota. Aff. of Eric Haskell (ECF #104) ¶ 3 & Exh. 1. In Initial Disclosures served on February 5, 2021, the plaintiff identified one employee of each designated manufacturer as knowledgeable about such artfully-framed topics as "[i]mpact of [Right to Repair] Law on vehicle safety and compliance . . . including potential safety hazards from disabling or reducing cybersecurity." Id. at Exh. 1.

On February 18, the plaintiff served two expert disclosures that, unsurprisingly, opined that manufacturers could not comply with the 2020 Right to Repair Law without eliminating existing cybersecurity controls built into vehicular design. Id. ¶ 4. The opinions expressed therein were premised on a generic vehicle design, purportedly shared by all "modern" vehicles, but explicitly tied to no particular make/model. Id. Nor did the sources cited by the plaintiff's experts include any primary technical documents evidencing the design of any particular make/model. Id. Rather, their sources consisted largely of high-level PowerPoint

presentations—at best, secondhand evidence of a vehicle's electronic and security design—as well as consultations with each designated manufacturer.[2] Id.

On February 22, now armed with the plaintiff's expert opinions and bases therefor, the Attorney General propounded her Second Set of Requests for Production (the "Requests"), which are attached to the Haskell Affidavit as Exhibit 3. Id. ¶ 6. The Requests specifically targeted the technical documents that the Attorney General had expected to receive with the plaintiff's expert disclosures, and that are necessary to evaluate the design and architecture of any vehicle manufactured by GM, FCA, Mercedes-Benz, or Toyota. Id. at Exh. 3. To tailor the Requests, the Attorney General selected only two makes/models for each designated manufacturer, and sought a limited set of documents for that make/model, including:

1. The .dbc or .arxml files, or other document describing supported CAN bus messages;
2. The security architecture diagram; and
3. All threat models and reports from previous security reviews.

See id.

Each of the requested documents has a commonly-understood meaning in the automotive industry—not unlike, say, the meaning of an "opinion" or a "transcript" in the legal industry. For example, .dbc and .arxml files each "describe[] permissible messages between and among an automobile's electronic control units or 'ECUs' (i.e., its internal processors), as well as the CAN bus networks (i.e., the most common type of network that connects those ECUs) over which

---

[2] Through an interrogatory response, the Attorney General learned the identities of the specific individuals with whom the plaintiff's experts had consulted; they included two employees of Toyota, two employees of Mercedes-Benz, four employees of GM, and one employee of FCA. See Haskell Aff. ¶ 5 & Exh. 2. Of those nine employees, only two had been identified in the plaintiff's initial disclosures. Compare id. Exh. 1 with id. Exh. 2.

those messages can be sent." Aff. of Craig Smith (ECF #102) ¶¶ 6-7. A security architecture diagram "is a common industry term that refers to a document that describes the security-related features and security-sensitive communications paths within the vehicle, including the various 'security boundaries' enforced by the vehicle, the security/trust relationships between internal systems, the mechanisms used to maintain those boundaries and relationships (e.g., diodes, secure gateways), and the mechanisms used to protect communications within the vehicle." Id. ¶ 8. And a security review is "a test of the security applied to a system," the report of which "commonly contain[s] information, in narrative form, about security boundaries and security architecture" and, importantly, "document[s] any faulty assumptions in the security network architecture or threat models." Id. ¶ 10.

The Attorney General requested that the plaintiff produce responsive documents within 30 days (i.e., by March 24). Haskell Aff. at Exh. 3. That "30 day" request was designed to balance the spirit of the Scheduling Order—which requires "good faith efforts to produce all non-privileged documents within 30 days of a document request," ECF #78 at 3—against the extremely short time (42 days) between service of the plaintiff's expert disclosures and the Attorney General's deadline to serve her expert disclosures. To underscore the point, counsel for the Attorney General advised plaintiff's counsel as early as March 1 that receipt of the requested documents was necessary for her to meet her expert disclosure deadline. Id. ¶ 7.

The plaintiff served its written responses to the Requests on March 9. Id. ¶ 8 & Exh. 4. Following a blizzard of objections, the plaintiff responded that it would produce documents responsive to each Request "after the parties meet and confer about the precise information sought . . . and the parties agree upon an appropriate means of producing and/or making responsive documents available for the Attorney General to review" in view of the "extreme

sensitivity of the information requested." Id. at Exh. 4. The Attorney General immediately arranged to meet with plaintiff's counsel to educate them about the meaning of common industry terms used in the Requests; that meeting took place on March 10 and was followed by an exchange of letters. See Id. ¶ 9 & Exhs. 5 & 6. As to the requested documents' sensitivity, the Attorney General pointed out that the documents would be produced pursuant to Protective Order (i.e., ECF #91), and that the plaintiff's claims "inherently require inquiry into sensitive matters of vehicular architecture." Id. at Exh. 5. Although the plaintiff refused to commit to producing responsive documents by March 24, the parties eventually agreed to continue the Attorney General's expert disclosure deadline to a date seven business days after completion of the plaintiff's production of documents in response to the Requests. Id. ¶ 10 & Exh. 7; see also ECF #78 at 4 (scheduling order permitting parties to make such agreements, so long as trial date and filing dates are unaffected). The plaintiff produced batches of documents in response to the Requests on March 23, March 24, March 25, and March 29. Id. ¶ 11.

On March 22, the plaintiff proposed to make certain documents—including the requested .dbc / .arxml files and security architecture diagrams—available for inspection "at the [manufacturers'] facilities here in the U.S." Id. ¶ 12 & Exh. 8. The Attorney General immediately sought details about this proposal. Id. ¶ 12. But, at a meeting held on March 23, plaintiff's counsel was unable to provide such basic information as: which manufacturer(s) proposed to require a site visit; or where, specifically, those proposed site visits would occur. Id. The Attorney General's subsequent request on March 31 for that same information was similarly fruitless. Id. ¶ 13 & Exh. 9.

Shortly before 5:00 P.M. on Friday, April 2, the plaintiff transmitted a letter announcing that its production was complete. Id. ¶ 14 & Exh. 10. It also declared that:

- FCA would make .dbc files available at a physical location in Troy, Michigan, on the condition that "[t]he Attorney General's representatives shall not copy, remove, or otherwise transfer any portion of those documents onto any recordable media or recordable device";

- GM would make .dbc and .arxml files,[3] along with a document that sounds like it depicts the 2020 Cadillac CT5's security architecture,[4] available at a physical location in Detroit, Michigan, on the same condition;

- Mercedes-Benz would make .dbc files available via an "electronic reading room," on the condition that "[t]he Attorney General's representatives shall not screen-capture, copy, remove, [download,] or otherwise transfer any portion of those documents onto any recordable media or recordable device"; and

- Toyota would not produce .dbc files, security architecture diagrams, certificate policies, threat models, or reports from previous security reviews, "which documents are owned by a non-U.S. Toyota company and fall outside the scope of the topics designated for [Toyota Motor North America's] testimony in AAI's Initial Disclosures."

Id. at Exh. 10. Although not announced in the April 2 letter, plaintiff's counsel subsequently admitted during the April 6 meet and confer preceding this motion that Mercedes-Benz had also withheld threat models, reports from previous security reviews, and possibly other documents that plaintiff's counsel was unable to identify, on the ground that they are in the possession, custody, or control of an overseas Mercedes-Benz affiliate. Id. at Exh. 11.

ARGUMENT

A party may seek to compel production of documents where "a party fails to produce documents or fails to respond that inspection will be permitted—or fails to permit inspection—as requested under Rule 34." Fed. R. Civ. P. 37(a)(3)(B)(iv). Here, the plaintiff has failed to produce documents necessary for the Attorney General to adequately develop the record in this

---

[3] Simultaneously, however, General Motors produced to the Attorney General "certain sample . . . DBC/ARXML files." Haskell Aff. at Exh. 10.

[4] The plaintiff has described this document only as "a document that provides a detailed list of signals, with transmitting and receiving control units specified, for the 2020 Cadillac CT5." Haskell Aff. at Exh. 10.

case. More specifically, the unproduced documents are necessary to analyze how the manufacturers' vehicles are designed, how those designs incorporate cybersecurity protections, and what opportunities the manufacturers might have to comply with the 2020 Right to Repair Law short of dismantling those protections. Accordingly, this Court should compel the plaintiff to produce the requested documents in a full and timely manner, so that the Court can evaluate the plaintiff's claims on a fully-developed record at trial in June.

A. This Court Should Compel the Plaintiff to Produce Responsive Documents, Instead of Insisting on "Read Only" Access to Those Documents or Requiring the Attorney General's Counsel and Experts to Travel to Michigan, During the Pandemic, to Inspect Them.

GM, FCA, and Mercedes-Benz have each announced that it will make certain documents available to the Attorney General and her experts only upon an "eyes only" condition. Haskell Aff. at Exh. 10. In addition, GM and FCA have each announced that it will make such "eyes only" documents available only at a physical location in Michigan. Id. These conditions are tantamount to a refusal to produce those documents, for three reasons.

First, the "eyes only" condition contravenes Rule 34. Where discoverable documents are not "produc[ed]" to a requesting party, Rule 34(a)(1) empowers the requesting party "to inspect, copy, test, or sample" those documents. The Rule's procedure extends beyond inspection, to include copying, testing, and sampling, for good reason: A party is entitled not just to "peek" at a discoverable document, but also to refer back to it, reconsider it, examine witnesses about it, and reevaluate it in light of later-acquired information—none of which would be possible under the plaintiff's unilateral "eyes only" condition here.

Second, the "eyes only" condition would be ineffective in the circumstances of this case. As Rule 34 anticipates, there are some discoverable documents, including electronically stored information, that require a party to be able to test and sample them to discern their meaning. The

.dbc and .arxml files at issue here fall into that category: Indeed, one of the Attorney General's experts has averred that, to make proper use of these files, he may well need to write custom code for them. Smith Aff. ¶ 13. Preventing the Attorney General's counsel and experts from copying, testing, and sampling these files will effectively prevent them from assessing the veracity of the plaintiffs' (and its experts') claims.

Even worse, the plaintiff has demanded that "eyes only" inspections for FCA and GM take place at physical locations in Michigan. In other words, it is the plaintiff's position that the Attorney General's unvaccinated counsel and expert must disregard CDC guidance and fly from Boston and Seattle, respectively, to sit in FCA and GM facilities and read these electronic documents in person. See Haskell Aff. ¶ 2, Smith Aff. ¶ 14. To insist on such unnecessary travel in the midst of a highly contagious and deadly pandemic violates common sense and basic fairness. See, e.g., Arnold v. City of Olathe, No. 18-2703-CM, 2020 WL 1847731, at *2 (D. Kan. Apr. 13, 2020) (in-person inspection of documents does not satisfy discovery obligations during COVID-19 pandemic; responding party must instead make "practical accommodations . . . to ensure [that the requesting party] obtains the documents to which he is entitled").

The plaintiff's insistence also dishonors this case's expedited discovery schedule, and the corresponding need for the parties to conduct discovery quickly and efficiently. As noted, the Attorney General propounded the Requests on February 22, the second business day after receiving the plaintiff's expert disclosures. The plaintiff first raised the possibility of an in-person inspection on March 22 yet, despite the Attorney General's repeated requests for more information, did not announce the location or any other details until April 2. Even now, the precise arrangements for such in-person inspections remain amorphous, contingent on further negotiations about "a mutually convenient date and time."

The only justification that the plaintiff has offered for this Byzantine and frankly dangerous method of "production" is confidentiality. But the very nature of the plaintiff's claim here requires inquiry into sensitive matters of vehicular architecture, if a meaningful record is to be developed for trial. And this Court has already addressed confidentiality concerns by issuing a Protective Order. As counsel for the Attorney General assured the plaintiff on March 11:

> [W]e are fully cognizant that these files are sensitive. We expect that you will designate these files 'confidential' or 'highly confidential' under the Confidentiality Protective Order (ECF # 91) as appropriate, and you should expect that we will treat them in accordance with that designation under the Confidentiality Protective Order.

Haskell Aff. at Exh. 5. In response, the plaintiff's counsel countered that "though we recognize that a Protective Order is in place, that hardly justifies producing this type of truly sensitive data when it is not at all clear that it is necessary," id. at Exh. 6—a position that the plaintiff had abandoned by April 2, when it conceded that the documents should be produced, but proposed a manner of "production" that is of no practical use to the Attorney General or the Court. Id. at Exh. 10. And, most tellingly, General Motors has already produced "sample" files of this type electronically, thereby undercutting any claim that an "eyes only" procedure is necessary.

B. This Court Should Compel Production of Documents Withheld By Toyota and Mercedes-Benz.

As noted, Toyota has withheld production of .dbc /.arxml files, security architecture diagrams, certificate policies, threat models, and reports from previous security reviews. Id. at Exh. 10. Mercedes-Benz has additionally withheld production of threat models, reports from previous security reviews, and possibly other documents that plaintiff's counsel is unable to identify. Id. ¶ 15.

These documents are manifestly discoverable. First, they are relevant to the plaintiff's claims. The plaintiff claims that the 2020 Right to Repair Law will require manufacturers to

"open up to third-party access sensitive electronic vehicle safety systems, including those that control steering, acceleration, and braking, and systems that control exhaust emissions," thus negating manufacturers' security measures, including "encryption keys, unique IDs, password protections, asymmetric keys or identity certificates exchanged between vehicle systems and a member's servers, authorized message requirements, secure boot, secure storage, network domain segregations, and firewalls." ECF #27 at 2, 12-13. Indeed, the plaintiff promised the Court at the Rule 12 motion hearing "[w]e're going to absolutely be able to develop the record. We're going to be able to have discovery and show Your Honor how the cyber and other protections are ingrained now in the vehicle system . . . ." ECF #94 at 39.

That is precisely the information that the plaintiff is now withholding. Specifically:

- .dbc and .arxml files "describe[] permissible messages between and among an automobile's electronic control units or 'ECUs' (i.e., its internal processors), as well as the CAN bus networks (i.e., the most common type of network that connects those ECUs) over which those messages can be sent. In other words, [they] describe[] what parts of the vehicle can talk to what other parts, and what they are allowed to say to each other." Smith Aff. ¶¶ 6-7.

- Security architecture diagrams "describe[] the security-related features and security-sensitive communications paths within the vehicle, including the various 'security boundaries' enforced by the vehicle, the security/trust relationships between internal systems, the mechanisms used to maintain those boundaries and relationships (e.g., diodes, secure gateways), and the mechanisms used to protect communications within the vehicle." Id. ¶ 8.

- Threat models are used by manufacturers to "identify and evaluate risk assumptions made in connection with designing a secure system." Id. ¶ 9.

- Security review reports "commonly contain information, in narrative form, about security boundaries and security architecture" and moreover "document any faulty assumptions in the security network architecture or threat models." Id. ¶ 10.

These documents are plainly relevant in view of the complaint specific allegation that the 2020 Right to Repair Law "may compromise the secure gateways between data stored onboard . . . and a vehicle's CAN bus," and "might require disabling CAN bus message filters and other means

used to segregate system components." ECF #1 ¶ 58. To develop a record on the plaintiff's claims, the Attorney General's experts must be able to examine, before providing opinions in this case, these technical documents that detail the vehicles' security measures.

Moreover, production of these documents is proportional to the needs of the case. See Fed. R. Civ. P. 26(b)(1). The Requests are carefully targeted, seeking only specific documents relating to two specified models for each manufacturer. The Requests are fully congruent with the concept discussed at the December 18, 2020, for developing a full record for trial:

> MR. HASKELL: [T]he concept is that the plaintiff is going to nominate, draft certain witnesses from among its membership and that discovery with respect to the facts those witnesses are going to be testifying to and putting forth is going to proceed as if the companies, the auto manufacturers they're employed by are parties to the case, and so there won't be issues of, 'It's not in our possession, custody or control,' or anything like that. Did we understand that correctly?
>
> THE COURT: That's the construct that I'm talking about here. You know, associational standing is somewhat odd but recognized, and I don't mean to permit the prospect of associational standing . . . to interfere with the full development of the information that's necessary. I would assume that no more than five companies and their representatives is sufficient to develop the question of associational standing and also to give you the opportunity to learn about and develop the questions of what their proprietary information is.
>
> * * *
>
> I think you're right on point on what I'm saying. That is, somebody doesn't say, 'Sorry, we didn't turn that over to the association.' Uh-huh. Assuming that it's something that I consider to be discoverable or is discoverable, you have to turn it over, as if, in your words, as if they were parties directing themselves -- or their companies were directing the parties.

ECF #79 at 16-17 (emphasis added).

The plaintiff has asserted two justifications for these categorical refusals to produce documents.[5] Neither has merit.

First, the plaintiff has asserted that the withheld documents "are owned by a non-U.S. Toyota company." But "ownership" is the wrong yardstick—what matters is whether the documents are "in the responding party's possession, custody, or control." Fed. R. Civ. P. 34(a)(1). And, "[u]nder Rule 34, 'control' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability, to obtain the documents . . . ." Calzaturficio S.C.A.R.P.A. v. Fabiano Shoe Co., Inc., 201 F.R.D. 33, 38 (D. Mass. 2001) (quoting Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000)); see also FM Generator, Inc. v. MTU Onsite Energy Corp., 2016 WL8902603, *3 (D. Mass Aug. 25, 2016) (That an entity can "secure documents of [an affiliate] to meet its own business needs," and has "access to documents when the need arises in the ordinary course of business," support a finding that the affiliate's documents are within the entity's control.). Here, it defies credulity to suggest that Toyota Motor North America, Inc., which describes itself as "the parent company for Toyota's marketing, sales, engineering and manufacturing arms in North America,"[6] lacks the ability to access design and architecture documents for Toyota vehicles sold in the United States. And, in fact, affidavits previously filed by the plaintiff in this case strongly suggest that it

[5] More precisely, it has offered two justifications for Toyota's withholding of these documents. As noted, the Attorney General learned only yesterday that Mercedes-Benz had similarly withheld documents.

[6] See https://www.toyotafinancial.com/us/en/investor_relations/about_toyota.html.

does not lack such access.[7] See ECF #43 ¶ 7 ("As part of its system of access and security controls, Toyota [defined to mean "Toyota Motor North America, Inc."] ensures the appropriate logical and physical isolation of vehicle control systems from external connections to provide layers of protection from cybersecurity threats . . . .") (emphasis added); id. ¶ 11 ("In order to attempt to comply with the Data Law's requirements by the timeframe contemplated in that law, Toyota would have no choice but to remove many existing access controls around vehicle systems.") (emphasis added).

Second, the plaintiff has asserted that the withheld documents "fall outside the scope of the topics designated for [Toyota Motor North America's] testimony in AAI's Initial Disclosures." But the scope of discoverable information is governed by Rule 26(b)(1), not by whatever limited points a party might list in its initial disclosures. Here, affidavits previously filed by the plaintiff in this case reveal that both David Stovall (the sole Toyota employee identified in the plaintiff's initial disclosures, who also consulted with the plaintiff's experts) and Stephen McFarland (a Toyota employee who was not identified in the plaintiff's initial disclosures, yet who also consulted with the plaintiff's experts) are knowledgeable about potentially discoverable information going far beyond the handful of topics listed in the plaintiff's initial disclosure. See generally ECF #43, ECF #46. In a similar way, both Thomas Grycz (the sole Mercedes-Benz employee identified in the plaintiff's initial disclosures) and Markus Rossman (a Mercedes-Benz "Manager, Connected Car & Telematics" who was not identified in the plaintiff's initial disclosures) are both sufficiently knowledgeable about

[7] Although common sense suggests the same conclusions as to Mercedes-Benz, Mercedes-Benz was not among the manufacturers who initially filed affidavits in connection with the preliminary injunction motion.

cybersecurity issues to have consulted with the plaintiff's experts. It is fundamentally unfair for the plaintiff to make these Toyota and Mercedes-Benz cybersecurity professionals available to consult with its experts, yet refuse to make available to the Attorney General and her experts the primary-source documents that are necessary to understand the cybersecurity design and functioning of Toyota and Mercedes-Benz vehicles.

C. This Court Should Compel Production of Responsive Reports of Security Reviews that Appear Not To Have Been Produced.

The plaintiff has emphatically declared that its production in response to the Requests is complete. See Haskell Aff. Exhs. 10 & 11. But the documents that the manufacturers have produced strongly suggest that there are responsive reports of security reviews that they have not yet produced.[8]

Setting aside Toyota and Mercedes-Benz—which, as discussed above, have expressly withheld reports of security reviews—documents produced in this case reveal [redacted]

[8] There may also be other responsive-but-unproduced documents of which the Attorney General is not yet aware.

[redacted] Even General Motors' public statements confirm that it "do[es] risk assessments as we go. We do it at the beginning to be sure that we apply the right security requirements. And we do it throughout as we do design reviews, implementation reviews, pen[etration] tests, and validation, we're constantly assessing the risk as we develop the vehicle." Smith Aff. ¶ 11.

[redacted] It once against defies credulity to assert that, for the four GM and FCA makes/models for which the Attorney General has requested documents, such a limited number of security reviews were ever conducted—and that all of those reviews occurred so recently. Reports of security reviews are crucial, not only because they "commonly contain information, in narrative form, about security boundaries and security architecture," but also because they "document any faulty assumptions in the security network architecture or threat models." As such, those reports are necessary to the analyze the plaintiff's contention that compliance with the 2020 Right to Repair Law necessarily means "eliminat[ing] existing cybersecurity controls that protect core vehicle functions . . . ." ECF #27 at 7.

CONCLUSION

For these reasons, the Attorney General respectfully requests that the Court grant her motion to compel.

Respectfully submitted,

ATTORNEY GENERAL
MAURA HEALEY

By her attorneys,

April 7, 2021

/s/ Eric A. Haskell
Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Assistant Attorneys General
Christine Fimognari, BBO No. 703410
Special Assistant Attorney General
Office of the Attorney General
One Ashburton Place
Boston, Mass. 02108
(617) 963-2589
eric.haskell@mass.gov

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the CM/ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on April 7, 2021.

/s/ Eric A. Haskell